TDL | Trust in Digital Life

Online Digital Signatures: Challenges and Opportunities

The Impact of the eIDAS and GDPR Regulations

March 2018

Contents

Executive Summary	3
Introduction	4
Offline Signatures	6
Online Signatures	8
Annex I: Trustseed's Implementation of Online Signatures	12

Executive Summary

To date company employees with their customers and suppliers managed, controlled and guaranteed their signature commitments by using offline physical and electronic means as well as their subcontracted operators.

In their offline management procedure, signatories were responsible for the security, compliance and legality of their unilateral commitment by electronic signature applied to the chosen file in their management software. They were also responsible for confidentiality and communication to counterparties.

Of the 240 billion documents signed and exchanged each year between companies, only 1% of documents were signed electronically (offline). The difficulty of managing multilateral and cross-border signatures, legal anomalies and frauds[1], the very high cost of transactions, and the lack of security and confidentiality in documentary communications are major drawbacks that justified the digital transformation into Cloud computing and led the European Commission to regulate the digital trust networks in the GDPR. Each digital trust network is based on advanced, online identity and documentary signature services offered to users by companies or professional communities; and these online services are qualified and certified by validation bodies through computer software conformity assessment and dynamic control of their traceability mechanisms in real time. Cloud computing contributes to the benefits and a 70% cost reduction by pooling the means of security, confidentiality, compliance, legality and interoperability, as well as support resources, maintenance and computing power.

A company offering trust services may outsource to qualified providers the processing of document, signature and consent originals, as well as the encrypted, nominative or pseudonymized communication of the original data transmitted to the management accounts, legal archiving chests and recipient management applications. All transactions are controlled in real time by traceability mechanisms (such as a private blockchain) supervised by a validation body that pre-emptively prevents users from anomaly or fraud, and delivers instantly each transaction or payment signed with the certificate of legal and fiscal value necessary for the registration in a digital balance sheet, and for the long-term administration of evidence enforceable against any third party.

The digital transformation market conforms to the GDPR (security, qualification, control) and to the eIDAS Regulation (advanced and validated signatures), represents overall, for certified software publishers and qualified service providers, an annual turnover of 54 billion EUR with an EBITDA greater than 35%.

1 According to ThreatMetrix 2016, 70% occurred within companies.

Introduction

Business leaders often charge themselves with responsibilities for selecting an e-signature solution without fully understanding the security implications. The integration of e-signature with existing security capabilities, especially with technology supporting customer and employee identity and access management (IAM), is essential for its success.

The offline electronic signature designed for workstation use in the Data Protection Directive (DPD)[2] is being transformed into an advanced online cloud-based solution according to both the eIDAS Regulation[3] and the General Data Protection Regulation (GDPR)[4]. In 2014 the eIDAS preamble declared that with respect to the DPD:

> *The offline signature offers no comprehensive cross-border and inter-sectoral framework for signing secure, reliable and easy-to-use electronic transactions.*

One of the general principles in law is that no one can pre-constitute evidence in his own favour. Electronic signatures apply to commitments made by bilateral or multilateral signatures of letters, contracts and transactions, subject to the legal requirements of the accounting, fiscal and professional dematerialization by codes of conduct. Each commitment by signature includes 20 document management functions which are subordinated to strong personal and professional security and rights validations as well as to compliance and legality controls (data and 'rules of the game').

2 Directive 1999/93/EC

3 eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation and a set of standards for electronic identification and trust services for electronic transactions in the European Single Market established in EU regulation No 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC with effect from 30 June 2016. It entered into force on 17 September 2014 and applies from 1 July 2016, except for certain articles listed in Article 52.

4 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation intended to strengthen and unify data protection for all individuals within the EU. It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the data protection directive (Directive 95/46/EC) of 1995. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

The validity and compliance criteria must be updated in real time on a multilateral basis in the Cloud between the parties and their providers in order to comply with the codes of conduct and establish incontestable numerical proofs. Only Cloud computing technology allows the intervention of a chartered control body (*Code of Conduct*) to verify in real time the validity of the rights of the parties in a digital transaction and the conformity of the associated document and signature originals in a context where the parties are domiciled with different trusted services, which may have qualified subcontractors, which in turn are different from each other and possibly located in different countries.

Only with Cloud computing will the GDPR and the eIDAS Regulation enable the EU to realise its vision of a Digital Single Market, which will generate savings of 415 M€[5].

5 In addition, it is important to consider that the reduction of IT costs has gone through four stages:
a. Software as a standalone application: all data centre and maintenance evolution costs
b. Business process outsourcing software: 20% reduction in data centre costs
c. Software as a service: 35% reduction except data centre and maintenance evolution reduction
d. Service as a result: 70% reduction in operation identity evidence value certification + full interoperability (mobility in collaborative management) + resilience.

Offline Signatures

In the offline electronic signature reformed by eIDAS, only the two "functions" of identity and signature are strong and qualified for a certain legal value: the first because it is delivered face-to-face with a certified identity; the second because identity rights are validated by an independent qualified certification authority.

For the other 18 functions handled offline by the signer on his workstation and in his own environment, rights validation and conformity checks are essentially distributed, visual, manual and often executed *a posteriori* and too late.

In the context of risks surrounding the offline signature, the signatory is judge and party: it cannot validly certify the probative value of its dematerialized transaction to each counterparty. Confidence in this kind of dematerialized transaction and offline signature is absolutely unreliable, for lack of exhaustive traceability and impartiality.

The legal archiving of the originals of the document and of the individual offline signatures affixed without a rigorous traceability sheet and without independent probative value certification in relation to the personal documentary process is not recommended in an electronic safe which does not restore documentary evidence, possibly questionable, than at the end of the lifetime of the document.

Offline counterparties, in this context of legal uncertainty, finally resort to the originals signed on paper. The offline signature prescribed in the DPD did not have an alternative to the certified qualified identity nor an alternative to the validation of an offline signature. The disadvantage of the usual offline signature is to impose on the parties an initial registration of their identity locally face-to-face (compulsory displacement, and subjects the counterparties to the entirely inadequate documentary dematerialization conditions of the Issuer.

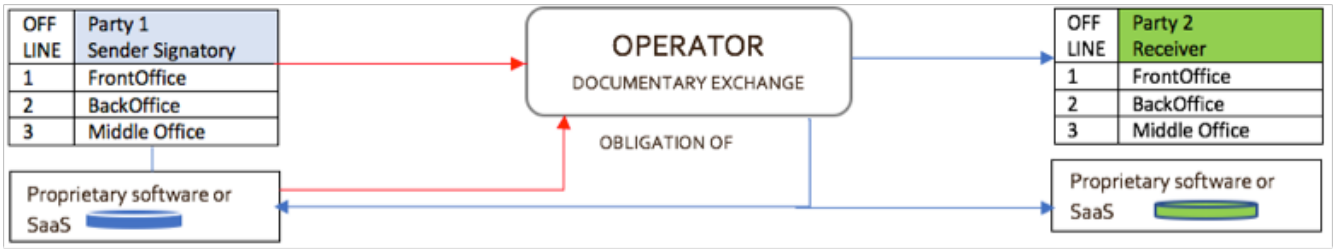

Figure 1:
Pre-2018 offline scheme

In other words, the signer could not use a verifiable substantial online identity without having to travel to a registrar to create his qualified digital identity certificate. The offline signature is also limited in its use since it is basically unilateral or univocal: it is not really interoperable with those of the other signatories engaged in the same transaction.

In other words, if several people want to sign the same document offline, it is not possible, nor is it certified as having probative value for all signatory parties. No signatory of the same document linked to other offline signatories can guarantee the end-to-end traceability with the other signatory parties responsible for each exchange of their personal and nominative signatures with the opposing parties.

Online Signatures

The need for online signatures is a huge market. Of the 240 billion letters and transactions signed each year, 99 % are signed manually, and less than 1% are signed with an offline signature which has the merit of being strong and qualified but is reduced to unilateral application.

However, as a result of the introduction of eIDAS and GDPR, the offline signature has been replaced by the online signature. These new provisions will make it possible to use a more practical signature the legal value of which will be substantial or sufficient in relation to the qualification standard.

The legal value of document and signature originals will be justified by a traceability sheet sealed in a blockchain. This documentary and multilateral legal value between parties will be guaranteed by an independent supervisory body of the national market authorities.

It is only within the framework of these two regulations that there is a solution for a substantial signature, the probative value of which is certain. The 20 dematerialized functions of management and documentary signatures are regulated for each correspondent or signatory, and for each type of correspondence.

Two functions remain under the exclusive control of users – identification and consent. The remaining 18 functions are entrusted and legally divided between qualified trust service providers (dedicated to identity privacy management, and service providers (dedicated to the creation of document and signature originals, all of them operating under the supervision of an independent supervisory body.

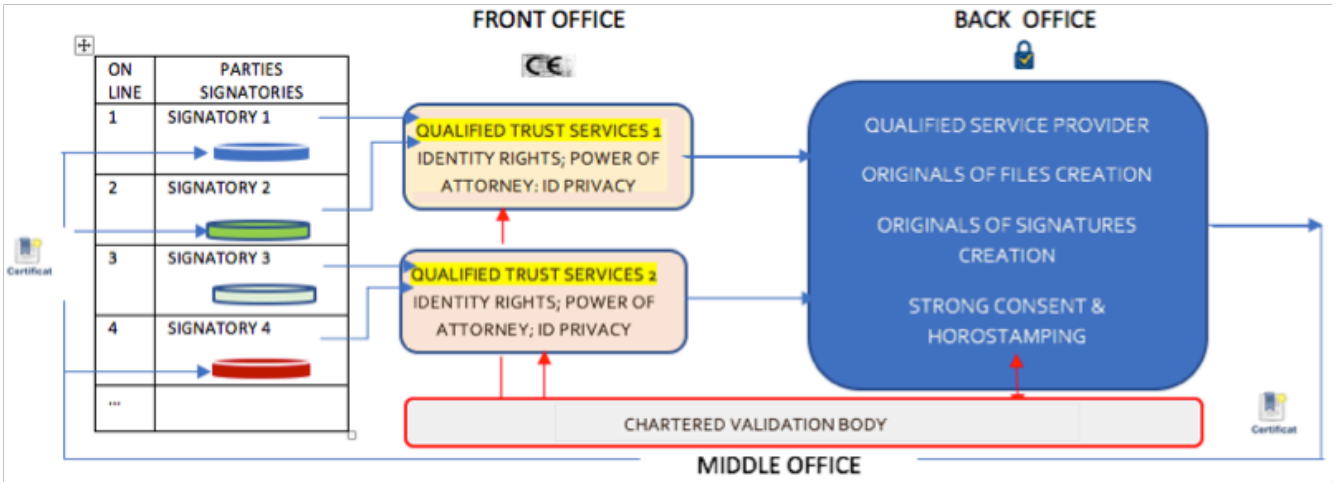

Figure 2:
2018 online scheme

The three disadvantages of the offline electronic signature are now overcome:

- Certification of the 20 digital functions of the documentary value chain (software, hardware, mechanisms of traceability sealed in blockchain),
- Impartiality and instantaneous validation of rights,
- Interoperability and resilience of procedures implemented between signatories and their original documents and digital signatures according to a code of conduct and interchange agreement.

For example, when three people want to sign a document, it requires three original registered documents, containing 3x3 or 9 original signed signatures of which each signatory keeps an original of the digital signatures created by each of the counterparties.

Between them, eIDAS and GDPR provide a solution that covers 99% of the market needs – for B2B and B2C – by making available to signatories of transactions and letters three types of interdependent operators that are specialized and autonomous:

- The responsible entity for qualified processing for trust services (identity and rights).

  The head of processing is normally a qualified legal body in a company who manages identity privacy for professional services and documentary accounts (employees, customers, suppliers).

- The service provider qualified in the creation of originals of documents and signatures online.

  The service provider is qualified for a code of conduct in the creation of document and signature originals for certain types of correspondence such as mail, transactions, payments, and financial instruments.

- The approved control body for the verification of data and for rights validations that must be continuously updated on the identity scoring lists, revocation / amendments list, qualified mandatory operator lists, certified feature- device lists, and lists of conventions interchange.

  This supervisory body is authorized to carry out, with respect to each code of conduct and each type of correspondence, the validation of the rights and the verification of the originals of documents and digital signatures on the basis of the consolidated traceability files sealed in a blockchain.

The strong dematerialization of signature commitments is now distributed and a variety of signature classes advanced to signatories in the Cloud: approximately 20% of the signatures will be qualified with a strong identity registered locally face-to-face and 80% of signatures will be measured and considered substantial from an online registration that includes a thorough and up-to-date verification of credentials and identity directories.

In both cases, the document management functions are dematerialized on behalf of each user or signatory between the person responsible for identity registration and the treatment of the services of trust and their subcontractors specialized in the originals of document and signature creation by codes of conduct and by types of correspondence.

The 20 document management functions are systematically subjected to the validation of rights[6] and to data conformity checks on documents and signatures before the administration of digital evidence by traceability files sealed in a blockchain.

This eco-system ensures the legal and informational security of any signature commitment by differently practising qualified or substantial signing either unilaterally or multilaterally, on a national or multinational basis.

The parties in correspondence and their signatories entrust mandates to someone responsible for the handling of trust services who subcontracts to service providers possessing a qualified device for the creation of document and signature originals.

Qualified trust services and their subcontractors (qualified processors) are subject to the verification of an approved supervisory body of the market authorities: this independent body is responsible for enforcing the obligations of result regarding the probative value of letters or transactions signed online.

Annex I: Trustseed's Implementation of Online Signatures

This analysis of the offline signature and its evolution towards a multilateral and certified online signature is essential for a good understanding of market issues, company expectations and the context in which TrustSeed obtained its first legal opinion in 2008 and the Award of Excellence in the area of Security and Confidence Architectures in 2016 from the European Commission[7].

This solution for dematerialization of originals of documents and signatures interfaces with all professional management software, either on premise or SaaS, and conforms with eIDAS and GDPR, the NIS Directive[8], the Data Protection Directive[9], as well as NSTIC[10].

The first version of TrustSeed's online signature was delivered by a Data Protection Officer and a subcontractor for document and signature creation, both of whom were subject to verification by an independent control body.

The new legal opinion concerning the multilateral cross-border digital signature platform and the commercial development of the safe digital confidence networks between companies and their customers take into account:

- The eIDAS articles relating to digital signature and the responsible for the treatment of confidential services[11];
- GDPR article 41, concerning the protection of personal data and the intervention of a control body. The chartered control body systematically reviews the validity of the identity rights and the conformity of the data required to certify the legal value of document and signature originals.

7 Corina Cretu, Commissioner for Regional Policy, Carlos Moedas, Commissioner for Research, Science and Innovation

8 The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services.9

9 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

10 The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a US government initiative announced in April 2011 to improve the privacy, security and convenience of sensitive online transactions through collaborative efforts with the private sector, advocacy groups, government agencies, and other organizations.

11 EU regulation no 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

In summary, the digital corporate signature platform allows the use of a substantial or qualified signature between several signatories of the same mail or transaction document.

Each document with its individual, digital and original signatures is managed by 20 document management functions, only two of which are under the control of the signatory (Identification and consent). The other 18 functions are under the control of qualified trust services managing identity rights and privacy with its subcontractor qualified for document and signature creation. These functions are systematically checked in real time by an independent control body regardless of their location in the Cloud.

Each online document management function relies on software system or on a certified hardware device subject to an average of 15 specific and instantaneous checks which are listed by a recording and traceability mechanism operating in a blockchain also certified by the chartered control body.

In total, in order to obtain certification of the probative value of a transaction, a letter or a payment, the registration of consolidated and sealed traceability records in a blockchain brings together 200 to 300 instant verification measures on all the 20 management and documentary signature functions that obey the specific constraints of each code of conduct and each type of correspondence mentioned in an official documentary repository.

trustindigitallife.eu

Trust in Digital Life Association
Maurice Dekeyserlaan 11 / Avenue Maurice Dekeyser 11
1090 Jette, Brussels
Belgium

office@trustindigitallife.eu
T +44 1738 583 533

TDL | Trust in Digital Life

trustindigitallife.eu

Trust in Digital Life Association
Maurice Dekeyserlaan 11 / Avenue Maurice Dekeyser 11
1090 Jette, Brussels
Belgium

office@trustindigitallife.eu
T +44 1738 583 533

TDL | Trust in Digital Life